

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS**

**IN RE: ARTHUR J. GALLAGHER DATA
BREACH LITIGATION**

This Document Relates To: All Actions

Master File No. 1:22-cv-00137

Consolidated Related Actions:
Case Nos. 1:21-cv-04056, 1:21-cv-04415,
1:21-cv-05851, 1:21-cv-04554

**MEMORANDUM OF LAW IN SUPPORT OF
GALLAGHER'S MOTION TO DISMISS THE CONSOLIDATED COMPLAINT**

TABLE OF CONTENTS

INTRODUCTION	1
BACKGROUND	4
I. The Ransomware Event and Gallagher’s Remedial Measures	4
II. The Parties	6
1. Defendants	6
2. Plaintiffs	6
LEGAL STANDARD	8
ARGUMENT	8
I. The Complaint Must Be Dismissed Because No Plaintiff Has Plausibly Alleged That Gallagher Breached Any Legal Duty (All Plaintiffs; Counts I-X, XII-XIV, and XVI)	8
II. The Complaint Must Be Dismissed Because No Plaintiff Plausibly Alleges a Causal Connection Between the Ransomware Event and Plaintiffs’ Injuries (All Plaintiffs; Counts I, II, V-VI, VIII-XV, XVII-XVIII)	11
III. Nine Plaintiffs Fail to Allege Cognizable Damages (Counts I-II, IV-V, VII-IX, XI-XV)	13
1. “Lost Time” Does Not Constitute Actual Damages	14
2. “Damage to” or “Diminution in Value of” PII Does Not Constitute Actual Damages	15
3. “Increased Risk” and “Anxiety” Do Not Constitute Actual Damages	16
4. Plaintiffs Caswell, Kroll, Horning, Owens, Mitchell, Myers, Parsons, Villalobos, and Wellikoff Fail to Allege Actual Damages	17
IV. Plaintiffs’ Data Breach Notification Statute Claims Fail To Allege Cognizable Harm (Counts VI, X, XI, XIII, XV, XVII)	18
V. Plaintiffs’ Attenuated Relationship to Gallagher Cannot Sustain Their Negligence, Contract, or Unjust Enrichment Claims (Counts I-III)	19
1. Plaintiffs Fail to Allege Any Common Law Duty of Care	19
2. Plaintiffs Fail To Allege Any Enforceable Implied Contract	19
3. Plaintiffs Conferred No Benefit That Unjustly Enriched Defendants (Count III)	21
VI. Plaintiffs’ California Law Claims Contain Additional Fatal Flaws (Counts IV-IX)	22
1. Plaintiff Myers Fails to State a Claim Under the CCPA (Count IV)	22

i.	Myers Has Not Pleaded Any Cognizable Claim.....	22
ii.	Myers Did Not Comply with CCPA’s Pre-Suit Notice Requirement.....	23
iii.	Plaintiff Myers Fails to Allege Facts That the Gallagher Defendants are Regulated “Businesses” Within the Meaning of the CCPA.....	23
2.	Plaintiff Myers Fails to State a Claim Under the CLRA (Count V).....	24
i.	Myers is Precluded from Seeking Damages Under the CLRA for Failure to Comply with CLRA’s Notice and Filing Requirements.....	25
ii.	Plaintiff Myers is Not a “Consumer” Qualified for Protection Under the CLRA.....	26
iii.	Plaintiff Myers Does Not Allege Any Qualifying Transaction Under the Statute.....	27
iv.	Plaintiff Myers Fails to Adequately Allege That His Damages Resulted From Gallagher’s Allegedly Unfair Practices	27
3.	Plaintiffs Cannot Bring CCRA Claims (Count VI)	28
4.	Plaintiffs’ Claims for Violation of the CMIA Fails (Count VII)	29
i.	The CMIA Claim Should Be Dismissed With Prejudice Because Plaintiffs Cannot Allege That Their Information Was Viewed By Unauthorized Individuals.....	29
ii.	Gallagher Is Not a Covered Entity Under Section 56.06 of the CMIA	30
iii.	Gallagher Is Not a Covered Entity Under Section 56.101 of the CMIA	31
iv.	Plaintiffs Are Not Entitled to Punitive Damages Under the CMIA Because Plaintiffs Cannot Allege that Gallagher Affirmatively Communicated PHI.....	31
5.	Plaintiffs’ UCL Claims Fails for Multiple Reasons (Counts VIII-IX)	32
i.	The UCL Lacks Extraterritorial Application	32
ii.	Plaintiffs Fail to Allege Causation and Reliance Under the UCL.....	33
iii.	Plaintiffs Fail to Allege “Unlawful” Conduct Under the UCL.....	34
iv.	Plaintiffs Fail to Allege “Unfair” Conduct under UCL	35
v.	Plaintiffs Are Not Entitled to the Relief They Seek Under the UCL.....	36

VII.	The Maryland Personal Information Protection Act Does Not Provide an Independent Right of Action (Count XIII)	38
VIII.	The Colorado Statutes Lack a Private Right of Action (Counts XVI, XVII)	38
IX.	Plaintiffs Fail to Allege an Intentional Act to Sustain Their Invasion of Privacy Claim (Count XVIII)	39
CONCLUSION.....		39

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Adams v. Cole Haan, LLC</i> , No. Sacv 20-913, 2020 WL 5648605 (C.D. Cal. Sept. 3, 2020)	36
<i>Aguilar v. Hartford Accident & Indem. Co.</i> , No. CV 18-8123-R, 2019 WL 2912861 (C.D. Cal. Mar. 13, 2019)	30
<i>Anderson v. Kimpton Hotel & Rest. Grp., LLC</i> , No. 19-CV-01860-MMC, 2019 WL 3753308 (N.D. Cal. Aug. 8, 2019)	10
<i>In re Apple & AT & T iPad Unlimited Data Plan Litig.</i> , 802 F. Supp. 2d 1070 (N.D. Cal. 2011)	26
<i>Archev v. Osmose Utilities Servs., Inc.</i> , No. 20-CV-05247, 2021 WL 3367156 (N.D. Ill. Aug. 3, 2021)	14, 20
<i>City of Arvada ex rel. Arvada Police Dep't v. Denver Health & Hosp. Auth.</i> , 403 P.3d 609 (Colo. 2017)	38
<i>Baba v. Hewlett-Packard Co.</i> , No. C 09-05946 RS, 2010 WL 2486353 (N.D. Cal. June 16, 2010)	34
<i>Backhaut v. Apple, Inc.</i> , 74 F. Supp. 3d 1033 (N.D. Cal. 2014)	35
<i>Bahari v. State Bar of Cal.</i> , No. 19CV360452, 2020 WL 5493870 (Cal. Super. Aug. 6, 2020)	23
<i>Becton, Dickinson & Co. v. Cytex Biosciences Inc.</i> , No. 18-CV-00933-MMC, 2019 WL 633008 (N.D. Cal. Feb. 14, 2019)	37
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	8
<i>In re Blackbaud, Inc., Customer Data Breach Litig.</i> , No. 20-mn-02972, 2021 WL 4866393 (D.S.C. Oct. 19, 2021)	21
<i>Buckley v. Santander Consumer USA, Inc.</i> , No. C17-5813 BHS, 2018 WL 1532671 (W.D. Wash. Mar. 29, 2018)	39
<i>In re Cap. One Consumer Data Sec. Breach Litig.</i> , 488 F. Supp. 3d 374 (E.D. Va. 2020)	21

<i>Cattie v. Wal-Mart Stores, Inc.</i> , 504 F. Supp. 2d 939 (S.D. Cal. 2007)	25
<i>Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.</i> , 20 Cal. 4th 163 (1999)	33
<i>Chambers v. American Trans Air</i> , 17 F.3d 998 (7th Cir. 1994)	8
<i>Community Bank of Trenton v. Schnuck Markets, Inc.</i> , 887 F.3d 803 (7th Cir. 2018)	19, 20
<i>Corona v. Sony Pictures Ent., Inc.</i> , No. 14-CV-09600 RGK EX, 2015 WL 3916744 (C.D. Cal. June 15, 2015)	14, 28
<i>Davidson v. Kimberly-Clark Corp.</i> , 889 F.3d 956 (9th Cir. 2018)	24
<i>Davis v. Nationstar Mortg., LLC</i> , No. 15-CV-02920-RS, 2016 WL 6822017 (N.D. Cal. Nov. 18, 2016)	14
<i>Doe v. SuccessfulMatch.com</i> , 70 F. Supp. 3d 1066 (N.D. Cal. 2014)	14
<i>In re Equifax, Inc., Customer Data Security Breach Litig.</i> , 362 F. Supp. 3d 1295 (N.D. Ga. 2019)	22
<i>In re Facebook Privacy Litig.</i> , 791 F. Supp. 2d 705 (N.D. Cal. 2011)	16
<i>Fox v. Iowa Health System</i> , 399 F. Supp. 3d 780 (W.D. Wisc. 2019)	18
<i>Fresno Motors, LLC v. Mercedes Benz USA, LLC</i> , 771 F.3d 1119 (9th Cir. 2014)	36
<i>Frezza v. Google Inc.</i> , No. 12-CV-00237-RMW, 2012 WL 5877587 (N.D. Cal. Nov. 20, 2012)	26
<i>Gibson v. Jaguar Land Rover N. Am.</i> , LLC, No. CV2000769CJCGJSX, 2020 WL 5492990 (C.D. Cal. Sept. 9, 2020)	35, 36
<i>In re Google, Inc. Privacy Policy Litig.</i> , 58 F. Supp. 3d 968 (N.D. Cal. 2014)	27
<i>Griffey v. Magellan Health Inc.</i> , No. CV-20-01282-PHX-MTL, 2021 WL 4427065 (D. Ariz. Sept. 27, 2021)	10, 15, 16

<i>Gustafson v. BAC Home Loans Servicing, LP</i> , No. SACV 11–915–JST, 2012 WL 4761733 (C.D. Cal. Apr. 12, 2012)	33
<i>Hadley v. Kellogg Sales Co.</i> , 243 F. Supp. 3d 1074 (N.D. Cal. 2017)	34
<i>Kearney v. Hyundai Motor Co.</i> , No. SACV 09-1298 DOC, 2010 WL 9093204 (C.D. Cal. June 4, 2010)	32
<i>Krottner v. Starbucks Corp.</i> , 406 F. App’x 129 (9th Cir. 2010)	17
<i>Kylie S. v. Pearson PLC</i> , 475 F. Supp. 3d 841 (N.D. Ill. 2020)	38
<i>Lawlor v. N. Am. Corp. of Illinois</i> , 983 N.E.2d 414 (2012)	38
<i>Lloyd v. Gen. Motors Corp.</i> , 397 Md. 108, 916 A.2d 257 (2007)	14
<i>Longenecker-Wells v. Benecard Services Inc.</i> , 658 F. App’x 659 (3d Cir. 2016)	20
<i>Maag v. U.S. Bank</i> , No. 21-CV-00031-H-LL, 2021 WL 5605278 (S.D. Cal. Apr. 8, 2021)	10
<i>In re Macbook Keyboard Litig.</i> , No. 18-cv-2813, 2020 WL 6047253 (N.D. Cal. Oct. 13, 2020)	36
<i>Madrigal v. Hint, Inc.</i> , No. CV1702095VAPJCX, 2017 WL 6940534 (C.D. Cal. Dec. 14, 2017)	36
<i>Meyer v. Sprint Spectrum L.P.</i> , 45 Cal. 4th 634 (2009)	27
<i>Morgan v. AT&T Wireless Servs., Inc.</i> , 177 Cal. App. 4th 1235 (2009)	25
<i>Moyer v. Michaels Store, Inc.</i> , No. 14-c-561, 2014 WL 3511500 (N.D. Ill. July 14, 2014)	16
<i>Norwest Mortg., Inc. v. Superior Court of San Diego Co.</i> , 72 Cal. App. 4th 214 (1999)	32
<i>O’Connor v. Ford Motor Co.</i> , No. 19-cv-5045, 2021 WL 4480743 (N.D. Ill. Sept. 30, 2021)	22

<i>Oliveria v. Aomoco Oil Co.</i> , 201 Ill. 2d 134 (2002)	11
<i>Outboard Marine Corp. v. Superior Ct.</i> , 52 Cal. App. 3d 30 (1975)	25
<i>Pagan v. Abbott Labs., Inc.</i> , 287 F.R.D. 139 (E.D.N.Y. 2012)	14
<i>Perkins v. LinkedIn Corp.</i> , 53 F. Supp. 3d 1190 (N.D. Cal. 2014)	33
<i>Phillips v. Apple Inc.</i> , No. 15-CV-04879-LHK, 2016 WL 5846992 (N.D. Cal. Oct. 6, 2016)	37
<i>Pisciotta v. Old Nat. Bancorp.</i> , 499 F.3d 629 (7th Cir. 2007)	16
<i>Ponder v. Pfizer, Inc.</i> , 522 F. Supp. 2d 793 (M.D. La. 2007)	14
<i>Pruchnicki v. Envision Healthcare Corp.</i> , 439 F. Supp. 3d 1226 (D. Nev. 2020), aff’d, 845 F. App’x 613 (9th Cir. 2021)	14, 15
<i>Purvis v. Aveanna Healthcare, LLC</i> , No. 20-cv-2277, 2021 WL 5230753 (N.D. Ga. Sept. 27, 2021)	21
<i>Regents of Univ. of Cal. v. Superior Court</i> , 220 Cal. App. 4th 549 (2013)	29
<i>San Miguel v. HP Inc.</i> , 317 F. Supp. 3d 1075 (N.D. Cal. 2018)	35
<i>Schertz v. Ford Motor Co.</i> , No. CV-20-3221, 2020 WL 5919731 (C.D. Cal. July 27, 2020)	36
<i>Sherman v. Ryan</i> , 331 Ill. Dec. 557 (App. Ct. 1st Dist. 2009)	21, 22
<i>Sitterli v. Csachi</i> , 344 Ga. App. 671 (2018)	22
<i>In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.</i> , No. 3:19-CV-2284-H-KSC, 2020 WL 2214152 (S.D. Cal. May 7, 2020)	18
<i>Sonner v. Premier Nutrition Corp.</i> , 971 F.3d 834 (9th Cir. 2020)	36

<i>In re Sony Gaming Networks and Customer Data Sec. Breach Litig. (Sony I)</i> , 903 F. Supp. 2d 942 (S.D. Cal. 2012).....	16, 35
<i>In re Sony Gaming Networks and Customer Data Sec. Breach Litig.</i> 996 F. Supp. 2d 942 (S.D. Cal. 2014).....	15
<i>Stearns v. Select Comfort Retail Corp.</i> , No. 08-2746 JF, 2009 WL 1635931 (N.D. Cal. June 5, 2009).....	25
<i>Sullivan v. Oracle Corp.</i> , 51 Cal. 4th 1191 (2011)	32
<i>Sutter Health v. Superior Court</i> , 227 Cal. App. 4th 1546 (2014)	29, 31
<i>Svenson v. Google Inc.</i> , No. 13-CV-04080-BLF, 2016 WL 8943301 (N.D. Cal. Dec. 21, 2016)	15
<i>Walters v. MedSouth Record Mgmt., LLC</i> , 38 So.3d 241 (La. 2010)	22
<i>Warner v. Tinder Inc.</i> , 105 F. Supp. 3d 1083 (C.D. Cal. 2015)	33
<i>White v. Citywide Title Corp.</i> , No. 18-CV-2086, 2018 WL 5013571 (N.D. Ill. Oct. 16, 2018)	39
<i>Willey v. J.P. Morgan Chase, N.A.</i> , No. 09-CV-1397, 2009 WL 1938987 (S.D.N.Y. July 7, 2009).....	17
<i>Williamson v. McAfee, Inc.</i> , No. 14-cv-00158-EJD, 2014 WL 4220824 (N.D. Cal. Aug. 22, 2014).....	35
<i>Willingham v. Global Payments, Inc.</i> , 1:12-CV-01157-RWS, 2013 WL 440702 (N.D. Ga. 2013).....	20
<i>Wofford v. Apple, Inc.</i> , No. 11-cv-0034-AJB (NLS), 2011 WL 5445054 (S.D. Cal. Nov. 9, 2011).....	37
<i>In re Yahoo! Customer Data Sec. Breach Litig. (Yahoo I)</i> , No. 16-MD-2752, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017)	16, 26
<i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.</i> , 313 F. Supp. 3d 1113 (N.D. Cal. 2018)	26
<i>Yu v. Int’l Bus. Machs. Corp.</i> , 314 Ill.App.3d 892 (2000)	14

Statutes

Cal. Bus. & Prof. Code § 17203	36
Cal. Bus. & Prof. Code § 17204	33
Cal. Civ. Code § 56.05.....	31
Cal. Civ. Code § 56.06.....	30
Cal. Civ. Code § 56.10.....	31, 32
Cal. Civ. Code § 56.26.....	31
Cal. Civ. Code § 56.35.....	31
Cal. Civ. Code § 56.101.....	30
Cal. Civ. Code § 1761.....	26, 27
Cal. Civ. Code § 1770(a)	24, 27
Cal. Civ. Code § 1780.....	25, 27
Cal. Civ. Code § 1782.....	25
Cal. Civ. Code § 1798.81.5.....	28
Cal. Civ. Code § 1798.82(b).....	28, 29
Cal. Civ. Code § 1798.140.....	23, 24
Cal. Civ. Code § 1798.150.....	9, 23, 34
Colo. Rev. Stat. § 6-1-713.5	38
Ga. Code Ann. § 10-1-912.....	19
La. Rev. Stat. Ann. § 51:3074.....	19
La. Rev.Stat. § 51:3075.....	18
Md. Code Ann., Com. Law § 14-3508	38
N.H. Rev. Stat. Ann. § 359-C:21	14
R.S.A. § 359-C:20(I)(a)	19

Other Authorities

*Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce,
Sci., & Transp.*, 109th Cong. 6 (2005).....10

Defendants Arthur J. Gallagher & Co. (“AJG”) and Gallagher Bassett Services, Inc. (“Gallagher Bassett”) (collectively, “Gallagher”), by and through their undersigned counsel, pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure and in support of their Motion to Dismiss, state as follows:

INTRODUCTION

This case arises from a criminal ransomware event that impacted Gallagher’s computer network systems in 2020 (the “Ransomware Event”). AJG and its subsidiaries provide insurance brokerage, consulting, and third-party claims settlement and administration services to businesses worldwide. Gallagher Bassett provides services relating to claim settlement, claim administration, and loss control. Plaintiffs are individuals whose personal information—primarily their names and insurance claim information—was potentially compromised during the Ransomware Event, typically because their employers engaged Gallagher’s business services.

The Complaint makes clear that criminal ransomware attacks are increasingly a fact of life for businesses, even for companies that devote significant resources to cybersecurity and work diligently to guard their network infrastructure. But Plaintiffs make three fundamental errors as to what should follow from this fact of life.

First, Plaintiffs do not plausibly allege any breach of duty. Alleging that a ransomware event occurred, without more, does not sufficiently or plausibly plead that Defendants acted negligently or breached a statutory duty of care. There is no such thing as perfect security, and when criminal actors are involved, breaches occur even when defendants have taken every reasonable precaution. As a result, both circuit and district courts have repeatedly concluded that the fact of unauthorized access alone is insufficient to allege that a defendant breached a duty to provide reasonable security measures. To sufficiently allege the breach of a legal duty, Plaintiffs must identify some specific, legally cognizable standard that wasn’t followed or procedure that

wasn't implemented. But Plaintiffs simply recite a laundry list of alleged best practices and further allege that, *because* the Ransomware Event occurred, Defendants necessarily must have failed to follow "one or more" of them. Compl. ¶¶66. This is insufficient as a matter of law, and dooms all of Plaintiffs' claims except for those based on invasion of privacy or violations of statutory notice requirements.

Permitting claims to proceed on such conclusory allegations of breach of duty would create perverse incentives and convert the legal framework applicable to data security incidents into a strict liability regime. This result would contradict the express intent of the nine state legislatures whose statutes Plaintiffs have placed in issue, who have enacted negligence rules through statutes mandating (at most) "reasonable" data security measures.

Second, Plaintiffs do not plausibly allege any causal connection between their purported harms and the Ransomware Event, let alone Defendants' conduct relating to that event. Ten of Plaintiffs' claims require a causal connection as a matter of law, but Plaintiffs' theory of causation is that data compromised in a ransomware event "can be" marketed via the dark web to other criminals, who then could potentially use the information to directly harm Plaintiffs through identity theft or similar crimes. But Plaintiffs have failed to plausibly allege such harm actually occurred because of *this* criminal Ransomware Event.

Plaintiffs generally do not allege that any of their information compromised in the Ransomware Event made its way to the dark web to be exploited by criminals. And there is a fundamental disconnect between the information allegedly compromised—primarily names and insurance claim information—and the privacy harms Plaintiffs allege to have suffered. For example, twelve Plaintiffs complain of increased spam calls, emails, or texts, and a handful allege unauthorized use of credit cards or online accounts. But not one of those alleges that any phone

number, email, username, password or credit card information was compromised in *this* Ransomware Event. Increased spam is endemic nationwide for reasons unrelated to data security. And the unauthorized use of credit card or account information that was not impacted in this Ransomware Event suggests (at most) that Plaintiffs' information may have been compromised in some unrelated incident—a conclusion confirmed by a basic search of public records. As such, Plaintiffs cannot plausibly allege that the Ransomware Event proximately caused them any injury.

Finally, Plaintiffs generally fail to allege any legally cognizable injury. Even if Plaintiffs had sufficiently alleged that Defendants' conduct somehow caused their alleged injuries, though they did not, not every irritation stemming from a cybersecurity incident is actionable. Ten of Plaintiffs' eighteen claims require plausible allegations of actual pecuniary harm, and the six statutory "delayed notice" claims require injury specifically attributable to the alleged delay. Nine plaintiffs fail the first requirement, alleging only that they suffered lost time, a theoretical risk of future harm, or a purported diminution of the value of their personal information, inconveniences consistently held insufficient to satisfy the duty to plead actual damages. And *none* of the Plaintiffs allege any harm resulting from the purportedly delayed notice, foreclosing their statutory notice claims. In sum, all of Plaintiffs' alleged common law and statutory claims fail to plausibly allege the essential elements of breach, causation, and/or harm.

In addition to these three fundamental problems, any one of which alone is dispositive, all of Plaintiffs' claims contain other fatal defects, addressed below in the order the claims are pled. For example, one California statutory claim is brought by a single plaintiff, about whom nothing is alleged other than his Los Angeles residence. Another plaintiff simultaneously claims both that he formed an implied contract with Gallagher regarding his personal information, and that he has no idea how his personal information ended up in Gallagher's possession. Three of the statutes

under which Plaintiffs sue provide no private right of action. Incredibly, the Complaint contains an intentional privacy tort even though there is no dispute that this action arises from a third-party criminal attack against Defendants. These defects are addressed beginning with Argument Part IV *infra*, and a chart summarizing the arguments by count follows this memorandum.

Ultimately, Plaintiffs allege nothing more than that a criminal ransomware event occurred and that they received notice some of their information was involved. For the numerous reasons that follow, no matter which legal theories are invoked, those allegations are simply insufficient to hold Gallagher liable. Thus, the Complaint should be dismissed entirely with prejudice.

BACKGROUND

I. The Ransomware Event and Gallagher's Remedial Measures

During the period from approximately June 3, 2020 to September 2020, third party criminals secretly accessed certain segments of Gallagher's network and installed Ragnar Locker ransomware on certain Gallagher systems. Ransomware is a type of malicious software, or malware, designed to encrypt files on a device and render the systems relying on such files unusable until a ransom is paid.¹ Upon discovering the Ransomware Event, Gallagher promptly took all its systems offline, initiated response protocols, notified law enforcement, launched an investigation with the assistance of third-party cybersecurity and forensic specialists, and implemented business continuity plans to minimize disruption to its customers and to ensure the ongoing security of its systems.²

In the days that followed, Gallagher negotiated with the threat actors to secure any exfiltrated data. On or around October 6, 2020, Gallagher reached a settlement with the threat

¹ The Cybersecurity and Infrastructure Security Agency, Ransomware, [WWW.US-CERT.CISA.GOV](https://us-cert.cisa.gov/Ransomware), <https://us-cert.cisa.gov/Ransomware> (last accessed December 4, 2021).

² <https://ajg.kroll.com/>.

actors. In exchange for payment, Gallagher received decryption keys, access to all exfiltrated data, confirmation that the threat actors did not retain any exfiltrated data, and confirmation that the threat actors did not (and would not) use any previously exfiltrated data against the individual data subjects, among other things.

The investigation confirmed which systems were accessed but could not confirm what specific information within those systems was actually accessed, so in an abundance of caution, Gallagher extensively reviewed the entire contents of the impacted systems.³ On May 24, 2021, Gallagher’s review of the contents of impacted servers confirmed that the impacted data included some personally identifiable information, or “PII,” and Gallagher worked to notify its business partners and obtain address information for impacted individuals to provide accurate notice to impacted parties.⁴

Although Gallagher is unaware of any actual or attempted misuse of personal information arising from the Ransomware Event, Gallagher offered identity and credit monitoring services for twenty-four months at no cost to those impacted by this incident, no matter what information was accessed.⁵ Gallagher is aware of no evidence that any data potentially accessed during the Ransomware Event was posted on the dark web, distributed to any third party, made public, or otherwise marketed for sale.

Following Gallagher’s announcement of the Ransomware Event, Plaintiffs brought several proposed class actions which were ultimately consolidated, asserting claims on behalf of themselves and a nationwide class comprised of “[a]ll United States residents whose PII and/or PHI [Protected Health Information] was accessed or acquired during the” Ransomware Event, as

³ *Id.*

⁴ *Id.*

⁵ *Id.*

well as nine subclasses (California, Colorado, Florida, Georgia, Illinois, Louisiana, Maryland, New Hampshire, West Virginia). *Id.* ¶¶ 276, 277–285. Plaintiffs assert claims for negligence, breach of implied contract, unjust enrichment, and invasion of privacy. *Id.* ¶¶ 300–352, 499–510. Plaintiffs also assert violations of the following state statutes: California’s Consumer Privacy Act (“CCPA”); California’s Consumers Legal Remedies Act (“CLRA”); California’s Customer Records Act (“CCRA”); California’s Confidentiality of Medical Information (“CMIA”); California’s Unfair Competition Law (“UCL”); Illinois’s Consumer Fraud and Deceptive Business Practices Act (“CFA”); Louisiana’s Database Security Breach Notification Law (“LDSBNL”); Maryland’s Consumer Protection Act (“MCPA”); Maryland’s Personal Information Protection Act (“MPIPA”); New Hampshire’s Consumer Protection Act (“NHCPA”); New Hampshire’s Notice of Security Breach statute; and Colorado’s Data Security and Breach Notification statutes. *Id.* ¶¶ 353–498.

II. The Parties

1. Defendants

AJG is “one of the leading insurance brokerage, risk management, and HR & benefits consulting companies in the world.” Compl. ¶ 2. Its group of companies includes Gallagher Bassett, a “Third-Party Administrator and claims manager that guide[s] [its] clients to improve their claims handling process, guard the reputation and financial interests of [its] clients, and go beyond expectations to accelerate resolution.” *Id.* ¶ 3. AJG and Gallagher Bassett are Delaware corporations with their principal places of business in Rolling Meadows, Illinois. *Id.* ¶ 42–43.

2. Plaintiffs

The Complaint names fifteen plaintiffs from nine states: Louisiana, California, Georgia, Florida, Illinois, New Hampshire, Maryland, Colorado, and West Virginia. Only two of these plaintiffs—Parsons and Yeremian—allege that they are former employees of a Defendant, whereas

the remaining plaintiffs do not allege any direct relationship with Gallagher. Compl. ¶¶ 96, 248. Furthermore, two of these plaintiffs—Caswell and Myers—do not allege what personal identifiable information of theirs was impacted by the Ransomware Event. *See id.* ¶¶119–129 (Caswell). The Complaint does not include a separate factual section for Myers at all.

Three of the named plaintiffs—Villalobos, Caswell, and Myers—allege they received notice of the Ransomware Event but do not allege they suffered any misuse of their personal information following the Ransomware Event. *See* Compl. ¶¶ 108–118 (Villalobos); 119–129 (Caswell). The remaining twelve plaintiffs allege various forms of misuse of their personal information since the Ransomware Event occurred, including alleged increase in the number of suspicious phone calls, emails, and text messages (*id.* ¶¶ 106, 134, 153, 159, 173, 196, 209, 220, 227, 240, 254, 273), unauthorized attempts to access bank accounts (*id.* ¶ 225), fraudulent charges on credit or debit cards or bank accounts (*id.* ¶¶ 159, 190, 267), email addresses posted on the dark web (*id.* ¶¶ 226, 240, 253), and attempts to open fraudulent accounts, claim unemployment or health insurance benefits, or file false tax returns (*id.* ¶¶ 172, 195, 241, 252). No Plaintiff, however, alleges that any of their phone, email, credit card, or online account information was compromised in the Ransomware Event. Compl. ¶¶ 99, 111, 122, 133, 146, 158, 170, 183, 202, 214, 224, 238, 251, 266. And Plaintiffs generally do not allege they suffered any actual economic losses as a direct result of the claimed misuse. Rather, Plaintiffs uniformly claim they suffered “lost time, annoyance, interference, and inconvenience,” as well as “a substantially increased risk” of future misuse of information and “diminution in value” of their personal information. *See, e.g., id.* ¶¶ 244–246. A handful of Plaintiffs also allege they suffered indirect economic harm associated with this alleged misuse, in the form of claimed mitigation expenses (*id.* ¶¶ 134, 220, 241, 259), late or

declined payment fees (*id.* ¶¶ 191-192), credit scores lowering (*id.* ¶¶ 135, 241, 255), or placing credit freezes (*id.* ¶¶ 136, 231, 241).

LEGAL STANDARD

To survive dismissal under Rule 12(b)(6), a complaint must articulate “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Dismissal is appropriate when a plaintiff fails to nudge his “claims across the line from conceivable to plausible” *Id.*

When considering a motion to dismiss a putative class action complaint, a court must consider allegations related to the named plaintiffs only, and not generalized allegations concerning unnamed plaintiffs or putative class members. *See also Chambers v. Am. Trans Air*, 17 F.3d 998, 1006 (7th Cir. 1994) (named plaintiff must have a valid cause of action in order to represent any proposed class).

ARGUMENT

I. The Complaint Must Be Dismissed Because No Plaintiff Has Plausibly Alleged That Gallagher Breached Any Legal Duty (All Plaintiffs; Counts I-X, XII-XIV, and XVI)

Virtually all of Plaintiffs’ claims require them to plausibly allege that Defendants committed some negligent or otherwise culpable act in connection with the Ransomware Event. Common law negligence (Count I), under any state’s law, requires breach of an applicable duty of care. Plaintiffs’ implied-in-fact contract claim (Count II) avers that Defendants promised to act “to help ensure an appropriate level of security for the PII [Personally Identifiable Information] and PHI [Protected Health Information].” Compl. ¶ 337. Plaintiffs’ unjust enrichment claim (Count III) also depends on the presumption that Defendants failed to provide “a reasonable level of security,” and that the money Gallagher purportedly saved by cutting unspecified corners constitutes unjust enrichment. Compl. ¶ 345. Plaintiffs’ statutory data privacy claims uniformly

require “a violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.” *E.g.*, Cal. Civ. Code § 1798.150(a)(1) (CCPA, Count IV). And Plaintiffs’ statutory unfair competition counts require proof either that Defendants violated an underlying privacy statute or that Defendants *falsely* represented that they would “employ reasonable measures that would have kept [individuals’] PII and PHI secure.” *E.g.*, Compl. ¶ 368. In short, all of these claims require Plaintiffs to sufficiently plead (and ultimately prove) that Defendants somehow fell short of some “reasonable” level of security: the breach of a cognizable legal duty of care.

To plausibly allege such a breach, Plaintiffs cannot simply assert that unauthorized access occurred—they must allege facts sufficient to show how Defendants’ data security measures were inadequate. Thus, in *Kuhns v. Scottrade, Inc.*, where class plaintiffs alleged only that that defendant “did not maintain sufficient security measures and procedures to prevent unauthorized access,” the Eighth Circuit held that such allegations did not plausibly allege the breach of any legal duty as required for plaintiffs’ tort, contract, and state consumer protection statutory claims: “[t]he implied premise that because data was hacked [Defendants’] protections must have been inadequate is a ‘naked assertion[] devoid of further factual enhancement’ that cannot survive a motion to dismiss.” 868 F.3d 711, 717-18 (8th Cir. 2017) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). District courts addressing the privacy and consumer protection statutes of California and other states have likewise dismissed complaints that fail to specify “which parts, if any, of [defendant’s] data security systems were below industry standards,” or that allege a laundry list of security standards without indicating “with which of the many standards listed” defendants did not comply. *Griffey v. Magellan Health Inc.*, No. CV-20-01282-PHX-MTL, 2021 WL 4427065, at *8 (D. Ariz. Sept. 27, 2021) (dismissing CCPA, California UCL, negligence, unjust

enrichment, and implied contract claims); *see also* *Maag v. U.S. Bank*, No. 21-CV-00031-H-LL, 2021 WL 5605278, at *2 (S.D. Cal. Apr. 8, 2021) (dismissing CCPA claim based on plaintiff’s “unsupported” and “conclusory” allegations that defendant did not “implement and maintain reasonable security procedures and practices,” “failed to effectively monitor its systems for security vulnerabilities,” and had “lax security”); *Anderson v. Kimpton Hotel & Rest. Grp., LLC*, No. 19-CV-01860-MMC, 2019 WL 3753308, at *5 (N.D. Cal. Aug. 8, 2019) (dismissing CCPA, California UCL, Colorado Consumer Protection Act, and contract claims because plaintiffs “fail[ed] to allege any facts in support of their conclusory assertion that” the defendant did not implement reasonable security protocols).

These cases persuasively acknowledge that a successful (criminal) cyber-attack, without more, does not plausibly plead negligence because “there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution.” *Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 109th Cong. 6 (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission); *see also* *Griffey*, 2021 WL 4427065 at *8 (“the existence of an adequate data security infrastructure and two data breaches in a year are not mutually exclusive”). Permitting non-cognizable claims to proceed to discovery whenever plaintiffs allege that their data was impacted by a criminal cyber-attack would effectively create a strict liability scheme for data privacy. This would contradict the express intent of the relevant legislatures, who uniformly expressed a preference for a negligence regime by enacting statutes mandating only “reasonable” security practices.

Nonetheless, Plaintiffs claim that the mere fact of a ransomware attack is sufficient to state a claim against Defendants for negligence. The Complaint summarizes a laundry list of recommended security practices, and then baldly concludes that the “occurrence of the Data

Breach indicates that Defendant[s] failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach.” Compl. ¶ 66. But Plaintiffs do not allege which (if any) of these alleged security practices Gallagher allegedly failed to follow, or how any such alleged failure caused the Ransomware Event. Again, the fact that the Ransomware Event occurred, by itself, does not show a breach of duty. Without more, Plaintiffs do not plausibly allege that Defendants breached any legal duty of care, whether arising under common law, contract, or statute. Accordingly, as a matter of law, all of Plaintiffs’ “duty of care” claims fail and must be dismissed.

II. The Complaint Must Be Dismissed Because No Plaintiff Plausibly Alleges a Causal Connection Between the Ransomware Event and Plaintiffs’ Injuries (All Plaintiffs; Counts I, II, V-VI, VIII-XV, XVII-XVIII)

Fourteen of Plaintiffs’ claims also require Plaintiffs to plead that Defendants’ allegedly improper conduct caused legal harm. Causation is axiomatically an element of common law negligence and contract claims. Similarly, the statutes require that plaintiff’s injury occur “as a result of” Defendant’s alleged statutory violation, imposing a proximate causation requirement. *See, e.g., Oliveria v. Aomoco Oil Co.*, 201 Ill. 2d 134, 149 (2002) (ICFA). Plaintiffs’ theory of causation is that the information compromised in a ransomware event “can be” marketed via the dark web to criminals who can use it to perpetrate identity fraud or other harms. Compl. ¶ 21. But Plaintiffs have not stated a claim unless they can plausibly plead their information was, in fact, misused in this fashion.

First, Plaintiffs fail to plausibly allege that their information from the Ransomware Event actually was posted to the dark web. Although Plaintiffs Wellikoff, Wilson, and Yeremian have baldly alleged (without more) that their data was posted to the dark web (Compl. ¶¶ 226, 240, 253), they fail to plausibly allege that this disclosure resulted from this specific Ransomware Event (rather than some other reason). Wilson and Wellikoff allege only that their email addresses are

on the dark web, but they do not allege that their email addresses were impacted in the Ransomware Event. Compl. ¶¶ 224, 226, 238, 240. Plaintiff Yeremian alleges that her telephone number, email address, and home address are among her PII on the dark web, but she does not allege that any of this information was accessed by the criminal actors during the Ransomware Event. Compl. ¶¶ 251, 253. The remaining twelve plaintiffs do not even attempt to allege that any of their data was posted to the dark web.

Second, Plaintiffs only allege harms that could *not* have been caused by the Ransomware Event. Most notably, twelve Plaintiffs allege an “increase” in spam calls, emails, and texts, but *none* of them allege that their phone numbers or email addresses were compromised in the Ransomware Event. Compl. ¶¶ 99, 106 (Parsons), 133, 134 (Davie), 146, 153 (Horning), 158, 159 (Kroll), 170, 173 (Marr), 183, 196 (McDonald), 202, 209 (Mitchell), 214, 220 (Owens), 224, 227 (Wellikoff), 238, 240 (Wilson), 251, 254 (Yeremian), 266, 273 (Bock). Similarly, Kroll and Wellikoff allege that only their names and medical claim information were impacted in the Ransomware Event. Compl. ¶¶ 157, 224. “Medical claim information” includes information like claim numbers, loss reserves, the state in which the insured resides, the state in which an accident occurred, and adjuster information. No logical connection exists between the compromise of this banal information and the “fraudulent charges” on Kroll’s credit card, or the unauthorized attempts to access Wellikoff’s Xfinity, GoDaddy, and bank accounts. Compl. ¶¶ 159, 225, 227. Similarly, the only data of Plaintiffs Owens and Bock exposed in the Ransomware Event were their names and medical information. *Id.* ¶¶ 214, 266. The disclosure of this information could not plausibly cause the “increase in spam phone calls” that led Owens to pay \$100 for a “spam phone system,” or Bock’s unauthorized debit card charges. *Id.* ¶¶ 214, 220. Plaintiff Caswell does not even allege what of his personal information was impacted in the Ransomware Event (*id.* ¶ 122), and Plaintiff

Myers alleges nothing at all. On this basis alone, these Plaintiffs' claims should be dismissed entirely for lack of causation.

Taken together, Plaintiffs allege only that (1) some of their information is on the dark web, but not the information that was actually impacted in the Ransomware Event; and (2) they are experiencing harms that were potentially caused by disclosure of particular information, but not the information affected by the Ransomware Event. Because Plaintiffs do not allege that their phone numbers or email addresses were compromised in the Ransomware Event, the alleged increase in spam certain Plaintiffs allege could only result from some unrelated disclosure, whether legitimate or unauthorized. And because no usernames, passwords, or credit card or bank account information were allegedly compromised, the purported misuse of credit cards or other online accounts suggests (at most) that some Plaintiffs' information was obtained via some other means. Plaintiffs do not claim otherwise, and a basic public records search reveals that Plaintiffs Bock, Caswell, Davie, Kroll, Marr, McDonald, Mitchell, Owens, Wellikoff, Wilson, Yeremian, and Parsons had their PII compromised in data breaches completely unrelated to Gallagher and that occurred prior to the Ransomware Event.⁶ Given the foregoing, Plaintiffs do not plausibly allege causation as a matter of law. Nor can they.

III. Nine Plaintiffs Fail to Allege Cognizable Damages (Counts I-II, IV-V, VII-IX, XI-XV)

Of the eighteen causes of action contained in the Complaint, ten require plaintiffs to plausibly allege actual pecuniary injury: (1) negligence; (2) breach of implied contract; and

⁶ A search of the Plaintiffs through websites such as “<http://www.truepeoplesearch.com>”, “<https://thatsthem.com>”, “<https://www.smartbackgroundchecks.com>”, and “<https://haveibeenpwned.com/>”, based on the information provided in the Complaint reveals that certain personal identifiable information of the Plaintiffs were compromised in data breaches that pre-dated and are not in any way related to the Ransomware Event.

violations of the (3) CLRA; (4) UCL; (5) CCRA, (6) ICFA; (7) LDSBNA; (8) MCPA; (9) NHCPA; and (10) New Hampshire Notice of Security Breach.⁷

Nine of the plaintiffs offer no allegations of harm beyond formulaic recitations of “lost time,” “damages to and diminution in the value of [their] PII,” an “increased risk of fraud” or other harm, and “annoyance, interference, and inconvenience.” *See, e.g.*, Compl. ¶¶ 103-115 (Parsons). As a matter of law, these allegations do not (and cannot) sustain claims under common law and statutes requiring actual injury. All of these claims are properly dismissed.

1. “Lost Time” Does Not Constitute Actual Damages

Courts have consistently held that, absent any out-of-pocket expenses, time spent obtaining credit reports or reviewing financial accounts does not constitute cognizable injury to sustain a claim arising from a data breach. *See, e.g., Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1233 (D. Nev. 2020), *aff’d*, 845 F. App’x 613 (9th Cir. 2021) (“[T]he court finds that tangible, out-of-pocket expenses are required in order for lost time spent monitoring credit to be cognizable as damages.”); *Corona v. Sony Pictures Ent., Inc.*, No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015) (“[G]eneral allegations of lost time are too speculative to constitute cognizable injury.”).

“Even when out-of-pocket expenses are alleged, Plaintiffs must also allege that the monitoring costs were reasonable and necessary.” *Griffey*, 2021 WL 4427065, at *6; *see also In*

⁷ *Yu v. Int’l Bus. Machs. Corp.*, 314 Ill.App.3d 892, 897 (2000) (negligence); *Archev v. Osmose Utilities Servs., Inc.*, No. 20-CV-05247, 2021 WL 3367156, at *2 (N.D. Ill. Aug. 3, 2021) (implied contract and ICFA); *Doe v. SuccessfulMatch.com*, 70 F. Supp. 3d 1066, 1075-76 (N.D. Cal. 2014) (CLRA and UCL); *Davis v. Nationstar Mortg., LLC*, No. 15-CV-02920-RS, 2016 WL 6822017, at *5 (N.D. Cal. Nov. 18, 2016) (“The CCRA, however, requires a showing of actual damages.”); *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 796 (M.D. La. 2007) (Louisiana Database Security Breach Notification Law); *Lloyd v. Gen. Motors Corp.*, 397 Md. 108, 916 A.2d 257, 277 (2007) (MCPA); *Pagan v. Abbott Labs., Inc.*, 287 F.R.D. 139, 149 (E.D.N.Y. 2012) (NHCPA requires personal, actual damages to institute a class action); N.H. Rev. Stat. Ann. § 359-C:21 (recovery in private action limited to actual damages).

re Sony Gaming Networks and Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 970 (S.D. Cal. 2014) (“In assessing whether credit monitoring services in the context of data breach cases are recoverable in negligence, courts . . . require a plaintiff to plead that the monitoring costs were both reasonable and necessary.”). Thus, even if Plaintiffs had offered a conclusory allegation that their out-of-pocket expenses were reasonable and necessary—which they have not—they would still need to properly allege that the free credit and identity monitoring services offered by Gallagher to those impacted by the criminal Ransomware Event were somehow inadequate to justify incurring the out-of-pocket expenses. No Plaintiff has done so.

2. “Damage to” or “Diminution in Value of” PII Does Not Constitute Actual Damages

All Plaintiffs claim that they suffered “damages to and diminution in the value of their PII.” *See, e.g.*, Compl. ¶¶ 103 (Parsons), 115 (Villabolos), 126 (Caswell). But “[c]ourts . . . recognize that merely alleging a diminution in value to somebody’s PII or PHI is insufficient” to allege cognizable injuries. *See Griffey*, 2021 WL 4427065, at *5. To state a claim premised on alleged diminution of value to PII, a plaintiff must allege that: (1) “a market exists for the personal information at issue”; and (2) an “impairment in [plaintiff’s] ability to participate in that market.” *Id.* (citing *Pruchnicki*, 439 F. Supp. 3d at 1234); *see also Svenson v. Google Inc.*, No. 13-CV-04080-BLF, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016). Here, the Complaint contains no allegations to address either of these requirements. The only “market” for PII that Plaintiffs reference is the illegal market on the “dark web.” Compl. ¶ 75. Because the dark web does not provide a legitimate market through which Plaintiffs could have sold their data, it cannot be used to support an allegation of decreased PII value. *Griffey*, 2021 WL 4427065, at *5. Without identifying a market in which they could have sold their data, and without alleging that they in fact

intended to do so, Plaintiffs Myers, Parsons, Caswell, Villalobos, Horning, and Mitchell cannot sustain a claim premised on an alleged loss in “value” of their PII or PHI. *Id.*⁸

3. “Increased Risk” and “Anxiety” Do Not Constitute Actual Damages

Allegations regarding an “imminent and impending injury arising from the increased risk of fraud, identity theft, and misuse resulting from [his or her] PII and PHI being placed in the hands of unauthorized third parties and possibly criminals” also do not constitute cognizable injury. Compl. ¶¶ 105, 117, 128, 152, 208. Courts routinely reject allegations of increased risk of identity theft as insufficient to state common law or statutory claims because the mere risk of future harm is not a cognizable injury. *See, e.g., Pisciotto v. Old Nat. Bancorp.*, 499 F.3d 629, 639 (7th Cir. 2007) (“Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.”); *Moyer v. Michaels Store, Inc.*, No. 14-c-561, 2014 WL 3511500, at *7 (N.D. Ill. July 14, 2014) (“Illinois courts have rejected the argument that an elevated risk of identity theft constitutes actual damage for purposes of stating common law or statutory claims.”); *In re Yahoo! Customer Data Sec. Breach Litig. (Yahoo I)*, No. 16-MD-2752, 2017 WL 3727318, at *22 (N.D. Cal. Aug. 30, 2017) (“Plaintiffs’ imminent risk of *future* costs as a result of the Data Breaches, although sufficient to establish standing under the broader-injury-in-fact requirements of Article III, is not sufficient to allege ‘lost money or property’ under the UCL.”) (emphasis in original); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig. (Sony I)*, 903 F. Supp. 2d 942, 970 (S.D. Cal. 2012) (collecting cases) (“[H]eightedened risk of identity theft, time and money spent on mitigation of that risk, and property value in one’s information, do not suffice as injury under the [California] UCL ... or the CLRA.”).

⁸ Under the California UCL, this theory is additionally flawed because the injury element of a UCL claim requires the loss of money or property, and “personal information does not constitute property for purposes of a UCL claim.” *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011).

Moreover, even where a plaintiff alleges misuse of personal information, such misuse does not constitute cognizable injury in the absence of actual, appreciable financial loss flowing from that misuse. *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010). In short, Plaintiffs' allegations regarding the risk of future harm and misuse of their data, absent any resulting out-of-pocket losses, are insufficient to sustain the statutory and common law claims.

Plaintiffs' allegations regarding "annoyance . . . anxiety and increased concerns," *e.g.* Compl. ¶ 219, do not constitute cognizable harm. As the increased risk of misuse is not cognizable in the abstract, the anxiety and annoyance stemming from this (non-actionable) risk also do not constitute actual injury. *See, e.g., Willey v. J.P. Morgan Chase, N.A.*, No. 09-CV-1397, 2009 WL 1938987, at *10 (S.D.N.Y. July 7, 2009) (dismissing claims because alleged damages related to anxiety, emotional distress, and loss of privacy all arose due to the "probability that [plaintiff's] data might have been misused" and thus did not qualify as actual damages).

Finally, Plaintiffs' alleged increase in "spam" calls or messages from third parties do not satisfy the injury requirement: although they may cause annoyance and lost time or increase the (theoretical) risk of future harm, such impacts do not constitute actual injury. And, as explained *supra* Part II, Plaintiffs do not allege any facts tying such phone calls, texts, or emails to the Ransomware Event.

4. Plaintiffs Caswell, Kroll, Horning, Owens, Mitchell, Myers, Parsons, Villalobos, and Wellikoff Fail to Allege Actual Damages

In light of the foregoing, nine named plaintiffs fail to plausibly allege the damages element of their claims. Three plaintiffs—Villalobos, Caswell, and Myers—rely solely on formulaic recitations of harm to plead damages and do not even attempt to plead facts that, if proven, would establish actual injury. Compl. ¶¶ 103-105 (Parsons), 115-117 (Villalobos), 126-128 (Caswell).

Plaintiffs Parsons, Horning and Mitchell allege an increase in spam texts and calls, (Compl. ¶¶ 106, 153, 209), but do not articulate any accompanying, out-of-pocket loss.

Finally, although Kroll, Wellikoff, and Owens allege fraudulent credit card charges, unauthorized attempts to access online accounts, and increased spam leading to the purchase of a \$100 “spam phone system” (Compl. ¶¶ 159 (Kroll), 225 & 231 (Wellikoff), 220 (Owens)), these harms have no causal link to Defendants’ conduct, *supra* Part II. Moreover, Plaintiffs fail to plead any allegedly attendant out-of-pocket losses arising from the alleged fraud. These deficiencies warrant dismissal as to these nine plaintiffs.

Accordingly, the individual claims for negligence and breach of implied contract, and for violations of CLRA, UCL, CCRA, ICFA, LDSBNA, MCPA, NHCPA, and New Hampshire Notice of Security Breach must be dismissed as to Plaintiffs Parsons, Caswell, Villalobos, Horning, Mitchell, Myers, Kroll, Wellikoff, and Owens.

IV. Plaintiffs’ Data Breach Notification Statute Claims Fail To Allege Cognizable Harm (Counts VI, X, XI, XIII, XV, XVII)

Plaintiffs attempt to plead claims based on California, Illinois, Louisiana, Maryland, New Hampshire, and Colorado statutes mandating timely disclosure of certain data security incidents. Because these statutes only regulate the timing of the notice, “Plaintiffs must allege incremental harm suffered as a result of the alleged delay in notification,” as opposed to harm from the incident itself. *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-CV-2284-H-KSC, 2020 WL 2214152, at *8 (S.D. Cal. May 7, 2020) (internal citations omitted); *Fox v. Iowa Health System*, 399 F. Supp. 3d 780, 801 (W.D. Wisc. 2019) (Illinois statute); La.Rev.Stat. § 51:3075 (permitting recovery only of “actual damages resulting from the failure to disclose in a timely manner”). Because Plaintiffs fail to allege any damages or incremental injury from the alleged delay in notification, these delayed notice claims are properly dismissed as a matter of law.

In addition, Plaintiffs' late notice claims based on the California and Colorado statutes also must be dismissed because these laws provide no private right of action under the circumstances alleged. *See infra* Parts VI.3 & VIII.

V. Plaintiffs' Attenuated Relationship to Gallagher Cannot Sustain Their Negligence, Contract, or Unjust Enrichment Claims (Counts I-III)

1. Plaintiffs Fail to Allege Any Common Law Duty of Care

At this stage, Plaintiffs' negligence claims require this Court to predict that the courts of nine separate states would recognize a "common law data security duty." *Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 816 (7th Cir. 2018). The Seventh Circuit has concluded that Illinois law would not recognize any such duty as to either former employees or commercial customers, relying primarily on the legislature's enactment of a data privacy statute requiring notice of a breach but no underlying duty to safeguard data. *Id.* Although the subsequent amendment of Illinois' legislation to impose a duty to implement "reasonable" security measures calls this decision into question as to Illinois law, the Seventh Circuit has yet to revisit it. Furthermore, this reasoning would also preclude recognizing a common law duty under the laws of Georgia, Louisiana, and New Hampshire, which exclusively impose a duty to notify, Ga. Code Ann. § 10-1-912, La. Rev. Stat. Ann. § 51:3074, N.H. R.S.A. § 359-C:20(I)(a), Colorado, which imposes both duties but does not provide a private right of action, *infra* Part VIII, and Florida and West Virginia, which impose neither duty.

2. Plaintiffs Fail To Allege Any Enforceable Implied Contract

Plaintiffs attempt to state an implied contract claim but allege no conduct from which any contract could be implied. An implied contract claim "must contain all of the elements of an express contract, along with mutual intent to contract," and these elements must be "inferred from the conduct of the parties in the milieu in which they dealt." *See, e.g., Archey v. Osmose Utilities*

Servs., Inc., No. 20-CV-05247, 2021 WL 3367156, at *2 (N.D. Ill. Aug. 3, 2021) (internal citations omitted) (applying Illinois law). Accordingly, where two parties do not deal with each other, no contract can arise. *See Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 820 (7th Cir. 2018) (implied data breach contract claim dismissed for lack of “direct” transaction between the parties).

Thirteen Plaintiffs allege no direct interactions with Gallagher, and they concede that Gallagher only obtained their personal information because their employers dealt with Gallagher. *See, e.g.*, Compl. ¶ 200 (“In connection with his employment with Circle Home, Inc., Plaintiff Mitchell entrusted his PII and PHI to Defendant, possibly through Defendant’s provision of workers’ compensation insurance to Circle Home, Inc. or its other business dealings with [Circle Home’s parent company].”) This indirect relationship, without more, cannot give rise to an implied contract as a matter of law. *See Willingham v. Global Payments, Inc.*, 1:12-CV-01157-RWS, 2013 WL 440702, at *20 (N.D. Ga. 2013) (dismissing an implied contract claim where plaintiffs did not provide their PII directly to Defendant).

The two remaining Plaintiffs—Parsons and Yeremian—allegedly provided personal information to Gallagher “in connection with [their] employment with” Gallagher. *See, e.g.*, Compl. ¶ 97. Nothing further is alleged, however, regarding these Plaintiffs’ relationship with Defendants. Although the Complaint quotes Gallagher’s December 2019 Privacy Policy, *id.* at ¶¶ 52-54, Plaintiffs do not allege that they provided their PII to Gallagher because they were relying on (or even knew of) Gallagher’s privacy policy or data security practices. Accordingly, Plaintiffs allege no facts that could give rise to an implied contract related to their data. *See Longenecker-Wells v. Benecard Services Inc.*, 658 F. App’x 659, 662 (3d Cir. 2016) (contract claim properly dismissed where plaintiffs alleged only that defendant “required Plaintiffs’ personal information

as a prerequisite to employment”); *Purvis v. Aveanna Healthcare, LLC*, No. 20-cv-2277, 2021 WL 5230753, at *15 (N.D. Ga. Sept. 27, 2021) (same).

3. Plaintiffs Conferred No Benefit That Unjustly Enriched Defendants (Count III)

Plaintiffs’ unjust enrichment claim fails because it relies on the unprecedented assertion that their PII is somehow inherently beneficial to Gallagher. Unjust enrichment claims uniformly require that the plaintiff confer a benefit on the defendant. *See, e.g., Sherman v. Ryan*, 331 Ill. Dec. 557, 578 (App. Ct. 1st Dist. 2009). Plaintiffs claim to have conferred a benefit because they provided Defendants with “their valuable PII and PHI.” Compl. ¶ 343. But PII is not inherently beneficial—it only supports an unjust enrichment claim when Defendants profit from its use or storage. *See, e.g., In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 413 (E.D. Va. 2020). Plaintiffs do not allege that Gallagher profited from the use or storage of their data. Rather, they claim that Defendants “enriched themselves by saving the costs they reasonably should have expended on data security measures.” Compl. ¶ 344. This does not make the PII a “benefit,” nor does it make the purported security savings a benefit *conferred by Plaintiffs*.

Furthermore, the thirteen non-employee Plaintiffs never provided Gallagher with their data at all. Where Plaintiffs never paid for or chose to utilize defendant’s services, but instead provided their PII to entities that used those services, unjust enrichment simply cannot apply. *In re Blackbaud, Inc., Customer Data Breach Litig.*, No. 20-mn-02972, 2021 WL 4866393, at *14 (D.S.C. Oct. 19, 2021) (distinguishing *In re Capital One* on these bases).

Unjust enrichment claims in Illinois, Louisiana, California, and Florida additionally require the absence of any other remedy at law, and are properly dismissed when, as here, the same facts are alleged to support statutory consumer protection claims. *See, e.g., O’Connor v. Ford Motor Co.*, No. 19-cv-5045, 2021 WL 4480743, at *28 (N.D. Ill. Sept. 30, 2021) (dismissing unjust

enrichment claims under California and Florida law); *Sherman v. Ryan*, 331 Ill. Dec. 557, 578 (App. Ct. 1st Dist. 2009) (Illinois law); *Walters v. MedSouth Record Mgmt., LLC*, 38 So.3d 241, 242 (La. 2010) (Louisiana law).

Finally, Georgia law also requires that the party who confers the benefit “must act with the expectation that the other will be responsible for the cost.” *Sitterli v. Csachi*, 344 Ga. App. 671, 673 (2018) (internal citations omitted). This expectation cannot be present where the data is not provided directly to a defendant but is acquired through third parties. *See In re Equifax, Inc., Customer Data Security Breach Litig.*, 362 F. Supp. 3d 1295, 1329-1330 (N.D. Ga. 2019). Here, because Georgia Plaintiff Caswell did not provide his data directly to Defendants (Compl. ¶ 120), his claim also fails for lack of this requisite expectation.

VI. Plaintiffs’ California Law Claims Contain Additional Fatal Flaws (Counts IV-IX)

1. Plaintiff Myers Fails to State a Claim Under the CCPA (Count IV)

Plaintiff Myers is the only California plaintiff who seeks to bring a claim under the CCPA on behalf of a California class. This claim fails as a matter of law because: (1) the Complaint contains no specific allegations about Myers whatsoever; (2) Myers did not comply with the CCPA’s pre-suit notice requirement; (3) the Complaint does not allege facts supporting the conclusion that Gallagher is a regulated “business” under the CCPA; and (4) Myers merely asserts conclusory allegations insufficient to state a claim under the CCPA.

i. Myers Has Not Pleaded Any Cognizable Claim

Unlike the other plaintiffs, the Complaint contains no allegations at all concerning Myers’ “experience.” Nothing is alleged as to whether and under what circumstances Myers provided any personal information to Gallagher, whether any such personal information was implicated in the Ransomware Event, or whether Myers has incurred any injury in connection with that Event. This

omission appears to be inadvertent but given this failure to plausibly allege any essential elements of his claims, Myers must be dismissed as a plaintiff entirely.

ii. Myers Did Not Comply with CCPA’s Pre-Suit Notice Requirement

The CCPA requires a consumer bringing an “individual or class-wide” claim, before “*initiating* any action,” to first “provide[] a business 30 days’ written notice identifying the specific provisions ... the consumer alleges have been or are being violated.” Cal. Civ. Code § 1798.150(b) (emphasis added). This 30-day period allows the business to cure the noticed violation and avoid liability for individual or class-wide statutory damages. *Id.*

Here, Myers alleges in conclusory fashion that he complied with the CCPA’s notice requirement, (*see* Compl. ¶ 360), but he does not attach the alleged notice or include any allegations in the Complaint indicating *when* he sent a written notice to Gallagher pursuant to Cal. Civ. Code § 1798.150(b). To the extent Myers purports to suggest some notice other than the initial complaint was sent, Gallagher is not aware of receiving any such notice from him. As such, Myers has failed to satisfy this prerequisite and his CCPA claim should be dismissed.

iii. Plaintiff Myers Fails to Allege Facts That the Gallagher Defendants are Regulated “Businesses” Within the Meaning of the CCPA

Plaintiff Myers’ CCPA claim depends on establishing that Gallagher is a “business” as defined by the CCPA, but Myers fails to allege any facts to support his conclusory allegation that Gallagher is a “business.” *See Bahari v. State Bar of Cal.*, No. 19CV360452, 2020 WL 5493870, at *3 (Cal. Super. Aug. 6, 2020) (finding that CCPA only applies to a business, as defined by §1798.140(c)). The CCPA creates a private right of action only against businesses, not service providers. *See* Cal. Civ. Code § 1798.150(a)(1). Since only the California Attorney General is authorized to bring civil legal claims under the CCPA against service providers, the CCPA claim against Gallagher must be dismissed. Cal. Civ. Code. § 1798.155(b).

Under the CCPA, only an entity that “collects consumers’ personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information” qualifies as a business. Cal. Civ. Code § 1798.140(c). On the other hand, an entity that “processes information on behalf of a business and” is a company “to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract” is a “service provider.” Cal. Civ. Code. § 1798.140(v). The Complaint is devoid of facts to support Myers’ conclusory allegations that either Defendant is a covered “business,” which is not surprising because Gallagher does not collect consumers’ data. To the extent that Gallagher receives and processes consumer information, it does so as a service provider to its customers. *See id.* Therefore, the Complaint states no cognizable CCPA claim against Gallagher.

2. Plaintiff Myers Fails to State a Claim Under the CLRA (Count V)

Plaintiff Myers is also the only California plaintiff who seeks to bring a claim under the CLRA on behalf of a California class, but his CLRA claim is similarly subject to dismissal for several independent reasons. The CLRA prohibits “unfair methods of competition and unfair or deceptive acts or practices ... undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to any consumer.” Cal. Civ. Code § 1770(a). CLRA claims sounding in fraud—like the one asserted in this action—are also subject to Rule 9(b)’s heightened pleading standard. *See Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956, 964 (9th Cir. 2018).

The theory of Myers’ CLRA claim is that Gallagher, in a transaction for “insurance services,” deceptively failed to disclose that its data network “was defective and/or insecure.” Compl. ¶ 365. Myers further alleges that he “would not have purchased insurance services or would not have paid the prices [he] paid for the insurance services” but for Gallagher’s “deceptive

acts and business practices.” *Id.* ¶ 369. The CLRA claim should be dismissed because Myers (i) did not comply with notice and filing requirements; (ii) is not a “consumer” qualified for protection under the CLRA; (iii) alleges no transaction subject to the CLRA; and (iv) fails to adequately allege actual reliance on any allegedly deceptive or misleading statements or that any damages resulted from Gallagher’s allegedly unfair practices.

i. Myers is Precluded from Seeking Damages Under the CLRA for Failure to Comply with CLRA’s Notice and Filing Requirements

California Civil Code section 1782(a) provides that, at least thirty days before a consumer may commence an action for damages under the CLRA, he or she is required to notify the prospective defendant “in writing” of the alleged violations and demand that they be cured. Cal. Civ. Code § 1782(a). “Failure to provide such notice prior will result in **dismissal of the claim with prejudice.**”⁹ *Stearns v. Select Comfort Retail Corp.*, No. 08-2746 JF, 2009 WL 1635931, at *15 (N.D. Cal. June 5, 2009) (emphasis added).

The Complaint alleges that Myers mailed the Section 1782 notice and Defendants failed to cure. Compl. ¶ 375. Notably, the Complaint does not specify when Plaintiff Myers mailed such notice, he did not attach the notice or proof it was sent, *id.*, and Gallagher has no record of having received such notice. Without a plausible allegation that Plaintiff Myers provided written notice in accordance with California Civil. Code section 1782 before initiating suit and gave Gallagher an opportunity to cure, the CLRA claim must be dismissed.

⁹ Some courts opine that the purpose of these requirements is to allow a defendant to cure and avoid liability, and that dismissal with prejudice is not necessary to further this purpose. *Morgan v. AT&T Wireless Servs., Inc.*, 177 Cal. App. 4th 1235, 1261 (2009). But these requirements were also adopted to “facilitate pre-complaint settlements of consumer actions wherever possible,” *Outboard Marine Corp. v. Superior Ct.*, 52 Cal. App. 3d 30, 41 (1975), and allowing Myers to sue first and notice later here would clearly “destroy the notice requirement’s utility.” *Cattie v. Wal-Mart Stores, Inc.*, 504 F. Supp. 2d 939, 950 (S.D. Cal. 2007).

In addition, Myers did not comply with California Civil Code section 1780, which requires a plaintiff pursuing a claim under the CLRA to “concurrently with the filing of the complaint,” to file an affidavit indicating that the plaintiff resides within the county in which the action was commenced or “where the transaction or any substantial portion thereof occurred.” Myers filed no such affidavit. Thus, the Court must dismiss the CLRA claim. Cal. Civil Code § 1780(d) (“If a plaintiff fails to file the affidavit required by this section, the court **shall** . . . dismiss the action...””) (emphasis added); *see also In re Apple & AT & T iPad Unlimited Data Plan Litig.*, 802 F. Supp. 2d 1070, 1077 (N.D. Cal. 2011) (dismissing CLRA claims in consolidated class action complaint because plaintiffs failed to provide required affidavits).

ii. Plaintiff Myers is Not a “Consumer” Qualified for Protection Under the CLRA

A CLRA plaintiff must plausibly allege that he is a “consumer,” meaning “an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes.” Cal. Civ. Code § 1761(d); *see also Frezza v. Google Inc.*, No. 12-CV-00237-RMW, 2012 WL 5877587, at *4 (N.D. Cal. Nov. 20, 2012). Myers only alleges, in conclusory fashion, that he “and the California Class are consumers within the meaning of Civ. Code § 1761(d).” Compl. ¶ 364. Myers has not alleged that he sought or acquired goods or services directly from Defendants (because he did not).¹⁰ To the extent that Myers argues he is a consumer because he provided his PII and PHI to purchase insurance services, (*see id.* ¶ 369), courts have repeatedly held that plaintiffs cannot “purchase” services with PII for purposes of the CLRA. *See Yahoo I*, 2017 WL 3727318, at *33 (collecting cases).

¹⁰ Myers’ initial complaint also failed to allege any relationship with Gallagher that would show a “consumer” transaction, further showing that leave to amend this claim would be futile.

iii. Plaintiff Myers Does Not Allege Any Qualifying Transaction Under the Statute

“The CLRA applies only to a limited set of consumer transactions, and is not a law of ‘general applicability.’” *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1141 (N.D. Cal. 2018). That statute applies to unfair practices by a “**person in a transaction** intended to result or which results in the **sale or lease of goods or services** to any consumer,” Cal. Civ. Code § 1770(a), and which thereby causes a plaintiff “damage,” Cal. Civil Code § 1780(a). Myers’ CLRA claim does not identify any specific “transaction” with Gallagher “for the sale or lease of” any good or service, much less the time, place, or manner as to when such a qualifying transaction might have taken place.

Moreover, the definitions of both “consumer” and “services” categorically exclude transactions made for “a commercial or business use,” rather than for personal, family, or household purposes. Cal. Civ. Code § 1761(b), (d). Myers alleges nothing about his purported transaction with Defendants and, as discussed *infra* Part VI.3, the other Plaintiffs only allege providing their information in the context of employment. Accordingly, the only conceivable transactions pleaded are business transactions outside the scope of the CLRA.

iv. Plaintiff Myers Fails to Adequately Allege That His Damages Resulted From Gallagher’s Allegedly Unfair Practices

In *Meyer v. Sprint Spectrum L.P.*, 45 Cal. 4th 634 (2009), the California Supreme Court made clear that a CLRA plaintiff must plead “tangible” harm. *Id.* at 640-43. Myers alleges only that he “would not have purchased insurance services or would not have paid the prices [he] paid for the insurance services” but for Gallagher’s “deceptive acts and business practices.” Compl. ¶ 369. But nowhere does Myers or any of the other California plaintiffs allege that they purchased insurance services from Gallagher. Nor does Myers allege that he actually read or heard the allegedly deceptive statements contained in Gallagher’s privacy policy prior to purchasing

insurance services. These deficiencies doom Myers' CLRA claim. *See In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 982-83 (N.D. Cal. 2014) (dismissing CLRA claim where plaintiff did not allege sufficiently that he had seen terms of Google's then-active privacy policy before creating his account because he "could not have relied on any representation it contained in making [his] decision[] to purchase" the good).

3. Plaintiffs Cannot Bring CCRA Claims (Count VI)

The CCRA requires businesses to "maintain reasonable security procedures and practices," Cal. Civ. Code § 1798.81.5, and provide notice of specified data breaches "immediately following discovery," Cal. Civ. Code § 1798.82(b). Plaintiffs' attempt to state claims under both provisions cannot succeed.

Under the CCRA, only a "customer"—"an individual who provides personal information to a business *for the purpose of purchasing or leasing a product or obtaining a service* from the business"—has a private right of action. *Corona v. Sony Pictures Ent., Inc.*, No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *7 (C.D. Cal. June 15, 2015) (quoting Cal. Civ. Code § 1798.80). Here, Defendants are an "HR & benefits consulting compan[y]" and a "Third-Party Administrator and claims manager." Compl. ¶¶ 2-3. Plaintiffs Parsons and Yeremian allege they provided their information in the course of their employment with Gallagher, *id.* at ¶¶ 97, 249, Wellikoff is unaware how his information was provided to Gallagher, *id.* ¶ at 223, and Myers alleges nothing. The remaining Plaintiffs allege vaguely that they provided their information to Defendants "[i]n connection with" their "employment" at various third parties, and that the information "possibly" went to Defendants in connection with insurance services provided to those third parties. *See, e.g., id.* at ¶ 144. Because the California Plaintiffs allege that they provided PII to Defendants or Defendants' customers as employees, *e.g., id.* ¶ 97, rather than customers, their CCRA claims must

be dismissed with prejudice in their entirety. *Corona*, 2015 WL 3916744, at *7 (dismissing CCRA claims of current and former employees impacted by Sony data breach).

Even if Plaintiffs had a right of action, their claims based on a failure to “implement and maintain reasonable security procedures and practices,” Cal. Civ. Code § 1798.81.5, do not plausibly allege breach, causation, or damages. *See supra* Parts I-III. And their claims based on failure to provide notice of a breach “immediately following discovery,” Cal. Civ. Code § 1798.82(b), do not allege any injury from any purported delay. *See supra* Part IV.

4. Plaintiffs’ Claims for Violation of the CMIA Fails (Count VII)

The California Plaintiffs allege violations of (1) CMIA provisions barring disclosure of medical information without prior authorization under Cal. Civil Code §§ 56.10, 56.11, 56.13, and 56.26, and (2) CMIA provisions forbidding negligent storage of medical information under Cal. Civil Code §§ 56.06 and 56.101. Compl. ¶¶ 397, 400. Neither claim can survive dismissal.

i. The CMIA Claim Should Be Dismissed With Prejudice Because Plaintiffs Cannot Allege That Their Information Was Viewed By Unauthorized Individuals

Plaintiffs’ CMIA claims must be dismissed because there is no violation of the CMIA unless an unauthorized person actually views the medical information. *See Regents of Univ. of Cal. v. Superior Court*, 220 Cal. App. 4th 549, 570 (2013). Thus, even where plaintiffs plausibly allege that computer components containing protected information were stolen, their claims fail absent some allegation that the thief actually viewed protected information. *Id.* (hard drive containing confidential medical information stolen); *see also Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1559 (2014) (computer containing confidential medical information stolen).

Here, the Complaint makes conclusory allegations that Plaintiffs’ information was “allowed” to have been viewed (but does not allege that it was actually viewed) by outside parties.

See, e.g., Compl. ¶ 395. This is insufficient to plead a violation of the CMIA. *See Regents*, 220 Cal. App. 4th at 570; *Sutter Health*, 227 Cal. App. 4th at 1559.

ii. Gallagher Is Not a Covered Entity Under Section 56.06 of the CMIA

Plaintiffs' claim pursuant to Section 56.06 fails as a matter of law for a fundamental reason—Gallagher is not a covered entity under this section. The California Plaintiffs allege that Defendants “are providers of healthcare, health care services plans and/or contractors for the purposes of this cause of action within the meaning of Civil Code § 56.06(a) and maintain medical information as defined by Civil Code § 56.05.” Compl. ¶ 390. Section 56.06 applies to any “business organized for the business of maintaining medical information” in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of healthcare, “for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual.” Cal. Civ. Code § 56.06(a). Plaintiffs have not alleged any facts to establish that Gallagher is a healthcare provider or in the business of maintaining medical information to make it available to individuals or health care providers. Indeed, at least one court has specifically held that insurance-related businesses like Gallagher are *excluded* from the CMIA. *Aguilar v. Hartford Accident & Indem. Co.*, No. CV 18-8123-R, 2019 WL 2912861, at *2 (C.D. Cal. Mar. 13, 2019) (dismissing CMIA claim because defendants were “workers compensation insurance carriers,” not providers of health care, health care service plans, or contractors as defined by the CMIA, and noting that “the CMIA expressly recognizes that an ‘insurance institution’ is not a contractor under the Act”). Thus, the California Plaintiffs fail to adequately allege that Gallagher is a covered entity under Section 56.06 of the CMIA.

iii. Gallagher Is Not a Covered Entity Under Section 56.101 of the CMIA

The California Plaintiffs also purport to state claims under Section 56.101 of the CMIA, which penalizes those who negligently maintain or store medical information. Compl. ¶ 400. Section 56.101 applies to a “provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information.” Cal. Civil Code § 56.101. The CMIA states a “provider of health care” is any “clinic, health dispensary, or health facility” licensed under certain California codes, and that a “health care service plan” is “any entity regulated pursuant” to certain California health and safety code statutes. *Id.* § 56.05(m), (f). A health care provider “does not include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code.” *Id.* § 56.05(m). Likewise, a contractor “does not include “insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code.” Cal Civ. Code § 56.05 (d). Thus, the California Plaintiffs cannot allege that Gallagher is governed by this provision, another reason the claim fails as a matter of law.

iv. Plaintiffs Are Not Entitled to Punitive Damages Under the CMIA Because Plaintiffs Cannot Allege that Gallagher Affirmatively Communicated PHI

Plaintiffs allege that “Defendants’ misuse and/or disclosure of medical information regarding Plaintiffs and California Class Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.” Compl. ¶ 397. Section 56.35 states that punitive damages can only be recovered by patients whose PHI has been used or disclosed in violation of sections 56.10, 56.104, 56.107, 56.20 or 56.26(a) and who have sustained economic loss or personal injury. Cal. Civil Code § 56.35. Plaintiffs, however, have not alleged a violation of any of these provisions. Under California law, in order to plead a violation of section 56.10(a), which mandates that health care providers and contractors shall not “disclose” medical information, a plaintiff must plead an

“affirmative communicative act” by the defendant, which does not occur if the information is stolen. *Sutter Health*, 227 Cal. App. 4th at 1556. Similarly, section 56.26 prohibits any person or entity engaged in the business of furnishing administrative services to programs that provide payment for health care services from **knowingly** using or disclosing medical information possessed in connection with performing administrative functions for a program, except as reasonably necessary. Cal. Civil Code § 56.26(a).

Here, Plaintiffs fail to plead any “affirmative communicative act” or knowing disclosure. Plaintiffs’ allegation that “Defendants knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties” to view PHI is purely conclusory and therefore insufficient as a matter of law to state a claim for violation of sections 56.10 or 56.26(a), foreclosing any alleged claim for punitive damages under section 56.35.

5. Plaintiffs’ UCL Claims Fails for Multiple Reasons (Counts VIII-IX)

Plaintiffs purport to bring claims on behalf of a nationwide class under California’s Unfair Competition Law (“UCL”).¹¹ These claims must be dismissed for the following reasons.

i. The UCL Lacks Extraterritorial Application

As a threshold matter, Plaintiffs’ UCL claims fail as a matter of law because California does not permit extraterritorial application of the UCL. *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011). Thus, the UCL may not be applied where, as here, the defendant’s headquarters and principal place of business are outside of California. *Norwest Mortg., Inc. v.*

¹¹ The Consolidated Complaint alleges that Count VIII: California’s Unfair Competition Law – Unlawful Business Practices is brought on behalf of the California Plaintiffs and the California Class, but alleges that “*Plaintiffs and the Nationwide Class seek relief under Cal. Bus & 17200, et seq.*” See Compl. ¶ 409 (emphasis added). Plaintiffs bring Count IX: California’s Unfair Competition Law – Unfair Business Practices on behalf of Plaintiffs and the Nationwide Class. Thus, for purposes of this Motion, Gallagher assumes that Plaintiffs purport to bring these UCL claims on behalf of a nationwide class. Plaintiffs’ UCL claims must be dismissed, however, for the reasons discussed herein.

Superior Court of San Diego Co., 72 Cal. App. 4th 214, 225 (1999); Compl. ¶¶ 42-43 (alleging AJG and Gallagher Bassett are incorporated under the laws of Delaware, with their headquarters and principal places of business in Rolling Meadows, Illinois).

Even if Defendants were based in California, though they are not, “a plaintiff may not assert an unfair competition claim against [a] corporation where the activities giving rise to the claim occurred outside California.” *Kearney v. Hyundai Motor Co.*, No. SACV 09-1298 DOC, 2010 WL 9093204, at *8 (C.D. Cal. June 4, 2010) (internal citations omitted). Here, the Complaint contains no allegation Gallagher’s purportedly wrongful conduct took place in, or emanated from, California. Because Plaintiffs do not (and cannot) plausibly so allege, their UCL claims fail as a matter of law. *Warner v. Tinder Inc.*, 105 F. Supp. 3d 1083, 1097 (C.D. Cal. 2015); *see also Gustafson v. BAC Home Loans Servicing, LP*, No. SACV 11-915-JST (ANx), 2012 WL 4761733, at *6 (C.D. Cal. Apr. 12, 2012) (finding the single allegation that “Defendants’ scheme was devised, implemented and directed from [their] offices in California” was “too vague to ‘plausibly suggest an entitlement to relief’ under the UCL”). Accordingly, Plaintiffs’ UCL claims (Counts VIII and IX) should be dismissed with prejudice.

ii. Plaintiffs Fail to Allege Causation and Reliance Under the UCL

Plaintiffs’ UCL claims are also properly dismissed because Plaintiffs fail to plead UCL’s causation and reliance elements to show they were injured “as a result of” any alleged unfair competition. Cal. Bus. & Prof. Code § 17204. None of the Plaintiffs allege when they came to rely upon any alleged misstatement by Gallagher, what that misstatement induced Plaintiffs to do, or what injury it caused to Plaintiffs. Because “actual reliance” is an essential element for UCL claims based on misrepresentations or nondisclosure, the UCL claim fails for this additional reason as well. *See Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1220 (N.D. Cal. 2014) (dismissing UCL claim for absence of allegations that plaintiffs actually read or relied on the alleged

misrepresentations that supposedly appeared on screens that all users had to click through to register for LinkedIn).

iii. Plaintiffs Fail to Allege “Unlawful” Conduct Under the UCL

The UCL “borrows violations of other laws and treats them as unlawful practices’ that the unfair competition law makes independently actionable.” *Cel-Tech Commc’ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999) (citations and quotations omitted). Plaintiffs allege that Gallagher’s conduct was “unlawful” based on purported violations of six statutes. None of these alleged violations can support a UCL claim.

Three of Plaintiffs’ predicate statutes are also alleged as stand-alone violations: the CCPA (Count IV); the CLRA (Count V); and the CCRA (Count VI).

As a threshold matter, the CCPA expressly prohibits Plaintiffs from using the CCPA as a UCL predicate. It states that “[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law.” Cal. Civ. Code § 1798.150(c). Moreover, Plaintiffs have not adequately pled a violation of any of these statutes. *See supra* Parts VI.1-3. “If a plaintiff cannot state a claim under the predicate law ... the UCL claim also fails.” *Hadley v. Kellogg Sales Co.*, 243 F. Supp. 3d 1074, 1094 (N.D. Cal. 2017) (brackets omitted).

The remaining “predicate” statutes are cited only in conclusory fashion in a single paragraph in support of Plaintiffs’ UCL claim (Count VIII): the California Financial Information Privacy Act, Cal. Fin. Code § 4052.5; the Graham Leach Bliley Act Privacy Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016; and Article 1, § 1 of the California Constitution.

Plaintiffs’ conclusory invocation of these remaining statutes, regulations, and the California Constitution, without any factual allegations whatsoever, is insufficient to state a UCL claim. In California, a “UCL claim of any kind must identify the particular section of the statute that was violated, and must describe with reasonable particularity the facts supporting the

violation.” *Baba v. Hewlett-Packard Co.*, No. C 09-05946 RS, 2010 WL 2486353, at *6 (N.D. Cal. June 16, 2010) (internal quotations and citations omitted). Because Plaintiffs do not “plead with particularity how the facts of this case pertain to that specific statute[,],” regulation, or section of California’s Constitution, Plaintiffs cannot base a UCL “unlawfulness” claim on these statutes, regulations, or California’s Constitution. *Id.*

iv. Plaintiffs Fail to Allege “Unfair” Conduct under UCL

Under California law, “unfair” conduct must satisfy either the “tethering test” and the “balancing test.” The “tethering test” requires “that the public policy which is a predicate to a consumer unfair competition action under the ‘unfair’ prong of the UCL must be tethered to specific constitutional, statutory, or regulatory provisions.” *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1051 (N.D. Cal. 2014). Under the “balancing test,” a business practice is unfair “if it is immoral, unethical, oppressive or unscrupulous and causes injury to consumers which outweighs its benefits.” *Id.* Where, as here, “unfair” practices claims rely on misrepresentations, Rule 9(b)’s heightened pleading standard applies. *See Sony I*, 903 F. Supp. 2d at 967.

Plaintiffs’ allegations do not satisfy either test, especially measured against Rule 9(b). Plaintiffs cannot “tether” their UCL claims to a violation of a “specific constitutional, statutory, or regulatory provision” because these predicate claims are insufficient. *See supra* Part VI.5.iii. Plaintiffs cannot avoid their pleading failures on these other claims by repleading the same allegations and calling them “unfair.” *See Backhaut*, 74 F. Supp. 3d at 1051 (dismissing unfair-prong claim tethered to Stored Communications Act because plaintiff failed to state a claim under that statute).

Plaintiffs fare no better on the balancing test. Plaintiffs plead no facts plausibly suggesting Gallagher’s acts were “immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers” and that the harm outweighs the utility of Gallagher’s acts. *San Miguel v. HP Inc.*,

317 F. Supp. 3d 1075, 1091 (N.D. Cal. 2018). Lacking “allegations that go towards comparing the harm to consumers against the utility of [Defendants’] conduct,” the UCL claim should be dismissed. *Williamson v. McAfee, Inc.*, No. 14-cv-00158-EJD, 2014 WL 4220824, at *7 (N.D. Cal. Aug. 22, 2014). Plaintiffs’ UCL claim premised on “unfair” conduct fails on these additional grounds.

v. Plaintiffs Are Not Entitled to the Relief They Seek Under the UCL

Remedies under the UCL are limited to restitution and injunctive relief, and do not include damages. *Gibson v. Jaguar Land Rover N. Am., LLC*, No. CV2000769CJCGJSX, 2020 WL 5492990, at *4 (C.D. Cal. Sept. 9, 2020); *see also* Cal. Bus. & Prof. Code § 17203. But a plaintiff cannot pursue these equitable remedies unless he can establish that he lacks an adequate remedy at law. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 845 (9th Cir. 2020) (affirming UCL claim dismissal of UCL claim where the plaintiff “fail[ed] to demonstrate that she lacks an adequate legal remedy”). Numerous courts have dismissed UCL claims in the wake of *Sonner* for that very reason.¹²

Here, Plaintiffs have not pled an inadequate legal remedy. On the contrary, Plaintiffs seek “damages, including actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined.” Compl., Prayer for Relief, D. Moreover, Plaintiffs’ UCL claim “relies upon the same factual predicates as [his] legal causes of action,” which seek money damages in connection with the Ransomware Event. *Madrigal v. Hint, Inc.*, No. CV1702095VAPJCX, 2017 WL 6940534, at *4-5 (C.D. Cal. Dec. 14, 2017) (quotation and

¹² *See, e.g., In re Macbook Keyboard Litig.*, No. 18-cv-2813, 2020 WL 6047253, at *4 (N.D. Cal. Oct. 13, 2020); *Gibson*, 2020 WL 5492990, at *3; *Schertz v. Ford Motor Co.*, No. CV-20-3221, 2020 WL 5919731, at *2 (C.D. Cal. July 27, 2020); *Adams v. Cole Haan, LLC*, No. Sacv 20-913, 2020 WL 5648605, at *2 (C.D. Cal. Sept. 3, 2020) (“The clear rule in *Sonner* [is] that plaintiffs must plead the inadequacy of legal remedies before requesting equitable relief[.]”).

citation omitted) (dismissing UCL and unjust enrichment claims because they rely on the same factual predicates as plaintiff's legal claims). In any event, Plaintiffs cannot argue that they are entitled to restitution or injunctive relief.

Even if the Complaint adequately pleaded Plaintiffs suffered loss of money or property (it does not), it alleges no such loss by Plaintiffs **to Gallagher**. See *Fresno Motors, LLC v. Mercedes Benz USA, LLC*, 771 F.3d 1119, 1135 (9th Cir. 2014) (“The restitutionary relief is limited to money or property lost by the plaintiff and *acquired by the defendant*.”) (emphasis added). Gallagher did not benefit financially from the criminal Ransomware Event, nor did Gallagher receive monies or property from Plaintiffs. Where, as here, a plaintiff does not “specify the source or the amount of the money” that he seeks and does not “allege any connection between the money [he] spent and money in [a defendant's] possession,” dismissal is appropriate. *Phillips v. Apple Inc.*, No. 15-CV-04879-LHK, 2016 WL 5846992, at *10 (N.D. Cal. Oct. 6, 2016). Moreover, because “[c]ase law is clear that the loss of use and loss of value ... are not recoverable as restitution because they provide no corresponding gain to a defendant,” Plaintiffs cannot use such a basis to support a claim for restitution. *Wofford v. Apple, Inc.*, No. 11-cv-0034-AJB (NLS), 2011 WL 5445054, at *3 (S.D. Cal. Nov. 9, 2011).

Plaintiffs are likewise not entitled to injunctive relief under the UCL. All of the Gallagher activity they allege to have been unlawful occurred in the past. See, e.g., Compl. ¶ 405 (“Defendants *engaged* in unlawful acts and practices ...”); ¶ 408 (“Defendants’ actions in engaging in the above-named unlawful practices and acts *were* negligent, knowing, and willful ...”) (emphasis added). Plaintiffs fail to allege how Gallagher’s alleged prior unlawful conduct “will probably recur” and thus fail to meet their burden of pleading facts to support a claim for injunctive relief under the UCL. See *Becton, Dickinson & Co. v. Cytex Biosciences Inc.*, No. 18-

CV-00933-MMC, 2019 WL 633008, at *7 (N.D. Cal. Feb. 14, 2019) (“Injunctive relief has no application to wrongs which have been completed, absent a showing that past violations will probably recur.”) (internal citation omitted).

VII. The Maryland Personal Information Protection Act Does Not Provide an Independent Right of Action (Count XIII)

Plaintiffs Owens and Wellikoff allege that Gallagher violated the MPIPA both as an independent claim and as part of their claim under the Maryland Consumer Protection Act. The MPIPA does not provide for a private right of action apart from an MCPA claim premised on a MPIPA violation, which Plaintiffs also plead. Compl. ¶ 440 (identifying violations Section 5 of the FTC Act and MPIPA as the predicate for their cause of action under the MCPA). Instead, a violation of MPIPA requirements “is an unfair or deceptive trade practice within the meaning of [MCPA]” and “is subject to the enforcement and penalty provisions contained in [MCPA].” Md. Code Ann., Com. Law § 14-3508. As Plaintiffs acknowledge, MPIPA “are subject to the enforcement and penalty provisions contained within the [M]CPA.” Compl. ¶ 456. Thus, Plaintiffs’ standalone MPIPA claim should be dismissed with prejudice.

VIII. The Colorado Statutes Lack a Private Right of Action (Counts XVI, XVII)

Plaintiff Wilson asserts that Gallagher’s actions violated Colorado’s statutes governing the protection of personal information, Colo. Rev. Stat. § 6-1-713.5, and requiring notice of a security breach, *id.* at § 6-1-716. These statutes, however, do not provide a private right of action; they only permit enforcement by the attorney general. *Id.* at § 6-1-716(4). The Colorado Supreme Court has held that if the Colorado General Assembly intends to confer a private right of action under a statute, it must state its intent “loud and clear,” by expressly “authorizing the remedy” in the statute itself. *City of Arvada ex rel. Arvada Police Dep’t v. Denver Health & Hosp. Auth.*, 403 P.3d 609, 614 (Colo. 2017). Because the statute does not do so, “the Colorado notification law

does not create a private right of action.” *Kylie S. v. Pearson PLC*, 475 F. Supp. 3d 841, 850 (N.D. Ill. 2020). Wilson’s Colorado statutory claims must be dismissed with prejudice.

IX. Plaintiffs Fail to Allege an Intentional Act to Sustain Their Invasion of Privacy Claim (Count XVIII)

Plaintiffs’ theory of invasion of privacy appears to arise from an intentional intrusion upon seclusion. Compl. ¶¶ 500-508. This theory requires allegations that Defendants “intentionally intrude[d]” upon Plaintiffs’ “solitude or seclusion.” *Lawlor v. N. Am. Corp. of Illinois*, 983 N.E.2d 414, 424 (2012) (quoting Restatement (Second) of Torts § 652B (1977)). Because Plaintiffs concede that Defendants were authorized to receive their private information, Compl. ¶ 505, this intrusion theory fails: there can be no “intrusion” if Defendants “possessed the necessary legal permission to acquire” Plaintiffs’ information. *Buckley v. Santander Consumer USA, Inc.*, No. C17-5813 BHS, 2018 WL 1532671, at *7 (W.D. Wash. Mar. 29, 2018). Plaintiffs cannot salvage this claim by recasting it as a wrongful disclosure to unauthorized parties. At a minimum, such claims require plausible allegations that Defendants “intentionally shared [Plaintiffs’] information with third parties.” *White v. Citywide Title Corp.*, No. 18-CV-2086, 2018 WL 5013571, at *3 (N.D. Ill. Oct. 16, 2018). Allegations that a defendant knew that its security measures were insufficient are not enough, and Plaintiffs offer nothing more. The Ransomware Event alleged involved an installation of malware on Defendants’ systems by third party criminals, and there is no allegation that Defendants intentionally took any action to assist this intrusion. Accordingly, this count fails as a matter of law and should be dismissed with prejudice.

CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court grant their motion and dismiss all of Plaintiffs’ claims against Defendants with prejudice. Defendants respectfully request such other, further relief as this Court deems just.

Respectfully submitted,

Dated: January 14, 2022

/s/ Livia M. Kiser

By: Livia M. Kiser

Livia M. Kiser

Jade R. Lambert

KING AND SPALDING LLP

110 N. Wacker Drive, Suite 3800

Chicago, IL 60606

lkiser@kslaw.com

jlambert@kslaw.com

(312) 995-6333 (telephone)

(312) 995-6330 (facsimile)

Stephanie A. Le (admitted *pro hac vice*)

KING & SPALDING LLP

633 West Fifth Street, Suite 1600

Los Angeles, CA 90071

sle@kslaw.com

(213) 443-4355 (telephone)

(213) 443-4310 (facsimile)

Counsel for Defendants

Arthur J. Gallagher & Co. and

Gallagher Bassett Services, Inc.

Summary of Argument: Motion to Dismiss in *In re Arthur J. Gallagher Data Breach Litigation*

COUNT		BASIS FOR DISMISSAL
Negligence (Count I) <i>All plaintiffs</i>		<ul style="list-style-type: none"> Failure to allege breach of duty or causation (all plaintiffs – Parts I & II) Failure to allege actual harm (nine plaintiffs* – Part III) Failure to allege duty (CO, FL, GA, IL, LA, NH, and WV Plaintiffs – Part V)
Implied Contract (Count II) <i>All plaintiffs</i>		<ul style="list-style-type: none"> Failure to allege existence of contract (all plaintiffs – Part IV) Failure to allege breach of duty or causation (all plaintiffs – Parts I & II) Failure to allege actual harm (nine plaintiffs* – Part III)
Unjust Enrichment (Count III) <i>All plaintiffs</i>		<ul style="list-style-type: none"> Failure to allege breach of duty or any benefit conferred (all plaintiffs – Parts I & IV) Failure to allege inadequacy of other remedies (CA, FL, LA, and IL Plaintiffs – Part IV) Failure to allege expectation that defendants would be responsible for costs (Caswell (GA) – Part IV)
CCPA (Count IV) <i>CA Plaintiff Myers</i>		<ul style="list-style-type: none"> Failure to allege any facts regarding plaintiff Myers (Myers – Part VI.1.i) Failure to allege breach of duty (Myers – Part I) Failure to provide required pre-suit notice (Myers – Part VI.1.ii) Failure to allege Defendants are regulated by the CCPA (Myers – Part VI.1.iii)
CLRA (Count V) <i>CA Plaintiff Myers</i>		<ul style="list-style-type: none"> Failure to provide required pre-suit notice (Myers – Part VI.2.i) Failure to allege consumer status or transaction (Myers – Part VI.2.ii-iii) Failure to allege breach, causation, or actual damages (Myers – Parts I.2.iv, II, & III)
CCRA (Count VI) <i>CA Plaintiffs[†]</i>	<i>Reasonable Security</i>	<ul style="list-style-type: none"> Failure to allege consumer status (CA Plaintiffs[†] – Part VI.3) Failure to allege breach of statutory duty or causation (CA Plaintiffs[†] – Parts I-II) Failure to allege actual damages (Myers & Villalobos – Part III)
	<i>Notice</i>	<ul style="list-style-type: none"> Failure to allege causation or consumer status (CA Plaintiffs[†] – Parts II, VI.3) Failure to allege actual damages from delay (Myers & Villalobos – Part III)
CMIA (Count VII) <i>CA Plaintiffs[†]</i>		<ul style="list-style-type: none"> Failure to allege unauthorized “viewing” (CA Plaintiffs[†] – Part IV.4.i) Failure to allege Gallagher is an entity covered under the CMIA (CA Plaintiffs[†] – Part IV.4.ii-iii) Failure to allege an affirmative act of disclosure (CA Plaintiffs[†] – Part IV.4.iv)
UCL (Counts VIII-IX) <i>CA Plaintiffs[†]</i>		<ul style="list-style-type: none"> No extraterritorial application (CA Plaintiffs[†] – Part IV.5.i) Failure to allege causation (CA Plaintiffs[†] – Part IV.5.ii) or damages (Myers/Villalobos – Part III) Failure to allege unlawful or unfair conduct (CA Plaintiffs[†] – Part IV.5.iii-iv) Failure to allege right to injunctive relief (CA Plaintiffs[†] – Part IV.5.v)
ICFA (Count X) <i>IL Plaintiff (Kroll)</i>		<ul style="list-style-type: none"> Failure to allege breach of duty as to “reasonable” precautions (Kroll – Part II) Failure to allege causation, actual damages and/or damages from delay (Kroll – Parts II-IV)
LDSBN (Count XI) <i>LA Plaintiff (Parsons)</i>		<ul style="list-style-type: none"> Failure to allege causation (Parsons – Part II) Failure to allege actual damages from delay (Parsons – Part III)
MCPA (Count XII) <i>MD Plaintiffs (Owens, Wellikoff)</i>		<ul style="list-style-type: none"> Failure to allege breach of duty as to “reasonable” precautions (Owens and Wellikoff – Part I) Failure to allege causation (Owens and Wellikoff – Part II) Failure to allege actual damages and/or damages from delay (Owens and Wellikoff – Parts III-IV)
MPIPA (Count XIII) <i>MD Plaintiffs (Owens, Wellikoff)</i>		<ul style="list-style-type: none"> No independent right of action— actionable only under MCPA (Owens and Mitchell – Part VII)
NHCPA (Count XIV) <i>NH Plaintiff (Mitchell)</i>		<ul style="list-style-type: none"> Failure to allege breach of statutory duty as to “reasonable” precautions (Mitchell – Part I) Failure to allege causation (Mitchell – Part II) Failure to allege actual damages and/or damages from delay (Mitchell – Part III)
NH statute: notice (Count XV) <i>NH Plaintiff (Mitchell)</i>		<ul style="list-style-type: none"> Failure to allege causation (Mitchell – Part II) Failure to allege actual damages from delay (Mitchell – Part III)
CO statute: reasonable security (Count XVI) <i>CO Plaintiff (Wilson)</i>		<ul style="list-style-type: none"> No private right of action (Wilson – Part VIII) Failure to allege breach of statutory duty (Wilson – Part I)
CO statute: notice (Count XVII) <i>CO Plaintiff (Wilson)</i>		<ul style="list-style-type: none"> No private right of action (Wilson – Part VIII) Failure to allege damages from delay (Wilson – Part V)
Invasion of Privacy (Count XVIII) <i>All plaintiffs</i>		<ul style="list-style-type: none"> Failure to allege causation or an intentional act (all plaintiffs – Parts II & IV.3)

* Caswell, Kroll, Horning, Owens, Mitchell, Myers, Parsons, Villalobos and Wellikoff.

† Davie, Marr, McDonald, Myers, Yeremian, and Villalobos

CERTIFICATE OF SERVICE

I hereby certify that on January 14, 2022, a true and correct copy of the foregoing document was filed through the Court's CM/ECF system. A copy will be sent electronically to all counsel of record by operation of the ECF system.

/s/ Livia M. Kiser
Livia M. Kiser